BBB WISE GIVING ALLIANCE & THE INTERNATIONAL COMMITTEE OF FUNDRAISING ORGANIZATIONS

BREACH OF DONOR DATA: BEYOND ONLINE SECURITY

ADVANCING TRUST IN THE CHARITABLE SECTOR CONFERENCE

June 12, 2015

Ellen Willmott
General Counsel & Corporate Secretary

The opinions expressed here are my own and not that of The Susan G. Komen Breast Cancer Foundation, Inc.
HYPOTHETICAL: IT'S FRIDAY AT 4 PM AND THE HEAD OF PROGRAM CALLS TO SAY – WE’RE GETTING LOTS OF ANGRY CALLS ABOUT A “SAVE THE DATE” POSTCARD SENT TO 10,000 SURVIVORS. WE DON’T KNOW WHY, HELP!
OTHER TYPES OF PROTECTED DONOR DATA

• A charity’s obligations to protect donor data extends beyond the protection of credit card and other financial information.

• Under most state law schemes regulating, “sensitive personal information” or “protected personal information” includes an individual’s name (or first initial with last name) in combination with:
  - The physical or mental health or condition of the individual;
  - The provision of health care to the individual; or
  - Payment for the provision of health care to the individual.

• Many charities, particularly those in social and health services, collect certain types physical health information, and may be subject to the same breach notification requirements.
REGULATION OF NON-FINANCIAL DONOR INFORMATION

• While not all states include personal health information in the definition of protected/sensitive information in the privacy/breach notification laws, many do (e.g. CA, FL, VA, TX)

• HIPAA (Health Insurance Portability and Accountability Act) also governs protected health information of employees/volunteers covered under a regulated health plan (HIPAA obligations are not discussed here)

• State breach notification laws are strict liability – intent is irrelevant

• PERKINS COIE (nationally ranked law firm) maintains an excellent chart on state security and privacy laws
WHAT IS THE RISK?

WHAT IS THE RISK TO YOUR CHARITY?

• Publicity regarding breach of security/privacy laws:
  – unauthorized access to the information (“unauthorized access of data in electronic form containing personal information”)
  – unauthorized use of sensitive personal information - even if the access is authorized (“access by an employee or agent of the [charity] is not a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use”)

• State law regulatory compliance
  – Charity is responsible for complying with breach notification requirements in each state in which affected individual resides
  – Third-party vendors maintaining databases may share in responsibility depending on type of breach and contract terms

• The charity spends valuable resources to comply with each state that regulates (italicized portions, excerpted from Fla. Stat. § 501.171)
WHAT DO WE DO?

• **Protect** “sensitive” personal information (encryption, restricted access, etc.)

• **Educate** staff that has access to such information on what uses are permitted

• **Review**, understand and coordinate check the information provided to donors/stakeholders at the point of collection (**REMEMBER**: a charity collects information from may sources: message boards/chat rooms, event registrations, donation forms, direct service/reference pages, business reply envelopes - what do you tell donors and stakeholders at each point of collection?

• **Implement** a response team/plan to manage
So, why would that hypothetical “Save the Date” card be problematic? WHAT IF POSTCARD SAID….

Mr. JOE SMITH  
#5 ANY STREET  
HOMETOWN, AA 00000  

Dear Mr. Smith,  
CONGRATULATIONS. IT IS TIME TO CELEBRATE YOUR VICTORY!!!

SAVE THE DATE: January 1, 2014  
OCCASION: CELEBRATING YOUR 5th YEAR AS A CANCER SURVIVOR  
WHERE: NEW LOCATION

The access to “survivor status” information may be authorized - BUT the use of that information in an unprotected mailer could be state law breach if the charity doesn’t have permission to publish the individual’s health status
CONCLUSION

• Know what information is considered “sensitive” “protected” and/or “personal information” for state law purposes – manage to the most restrictive state

• Understand what donors/stakeholders are told at the point of collection (in every format)

• Use commercially reasonable measures to protect the information

• Educate those with access to protected information on what may and may not be done with that information

• Have a response team/plan in place to manage a breach situation